Cisco Identity Services Engine Troubleshooting Guide, Release 1.0.4

Revised: March 18, 2013, OL-25997-01

Contents

This document provides several categories of troubleshooting information to assist in identifying and resolving problems you may encounter when you use the Cisco Identity Services Engine (ISE). This document contains the following sections:

- Installation and Network Connection Issues, page 2
- Licensing and Administrator Access, page 8
- Configuration and Operation (Including High Availability), page 9
- External Authentication Sources, page 12
- Client Access, Authentication, and Authorization, page 17
- Error Messages, page 31
- Configure NADs for ISE Monitoring, page 35
- Troubleshooting APIs, page 36
- Contacting the Cisco Technical Assistance Center, page 36
- Documentation Updates, page 37
- Related Documentation, page 38
- Obtaining Documentation and Submitting a Service Request, page 39

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Installation and Network Connection Issues

If you believe you are experiencing hardware-related complications, first verify the following on all of your deployed Cisco ISE nodes:

- The external power cable is connected, and the proper power source is being applied.
- The external cables connecting the appliance to the network are all secure and in good order.
- The appliance fan and blower are operating.
- Inadequate ventilation, blocked air circulation, excessive dust or dirt, fan failures, or any environmental conditions that might affect the power or cooling systems.
- The appliance software boots successfully.
- The adapter cards (if installed) are properly installed in their slots, and each card initializes (and is enabled by the appliance software) without problems. Check status LEDs on the adapter card that can aid you identifying a potential problem.

For more information on Cisco ISE hardware installation and operational troubleshooting, including power and cooling requirements and LED behavior, see the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.0.4*.

Tip For issues regarding potential network access device (NAD) configuration issues, including AAA, RADIUS, profiler, and web authentication, you can perform several validation analyses by choosing the Cisco ISE **Monitor > Troubleshoot > Diagnostic Tools > General Tools > Evaluate Configuration Validator** options.

Current Installation and Network Connection Troubleshooting Topics

- Unknown Network Device, page 3
- CoA Not Initiating on Client Machine, page 3
- Users Are Assigned to Incorrect VLAN During Network Access Sessions, page 3
- Client Machine URL Redirection Function Not Working, page 4
- Cisco ISE Profiler is Not Able to Collect Data for Endpoints, page 5
- RADIUS Accounting Packets (Attributes) Not Coming from Switch, page 5
- Policy Service ISE Node Not Passing Traffic, page 6
- Registered Nodes in Cisco ISE Managed List Following Standalone Reinstallation, page 7
- Primary and Secondary Inline Posture Nodes Heartbeat Link Not Working, page 7

Unknown Network Device

Symptoms or Issue	Cisco ISE is not able to identify the specified Network Access Device (NAD).
Conditions	Click the magnifying glass icon in Authentications to display the steps in the Authentication Report. The logs display the following error message: • 11007 Could not locate Network Device or AAA Client Resolution
Possible Causes	The administrator did not correctly configure the network access device (NAD) type in Cisco ISE.
Resolution	Add the NAD in Cisco ISE again, verifying the NAD type and settings.

CoA Not Initiating on Client Machine

Symptoms or Issue	Users logging into the Cisco ISE network are not experiencing the required Change of Authorization (CoA).
Conditions	Cisco ISE uses port 1700 by default for communicating RADIUS CoA requests from supported network devices.
Possible Causes	Cisco ISE network enforcement points (switches) may be missing key configuration commands, may be assigning the wrong port (i.e., a port other than 1700), or have an incorrect or incorrectly entered key.

Resolution	Ensure the following commands are present in the switch configuration file (this is required on switch to activate CoA and configure):
	`aaa server radius dynamic-author`
	`client <Monitoring_node_IP_address> server-key <radius_key>`

Users Are Assigned to Incorrect VLAN During Network Access Sessions

Symptoms or Issue	Client machines are experiencing a variety of access issues related to VLAN assignments.

Conditions	Click on the magnifying glass icon in Authentications to launch the Authentication Details. The session event section of the authentication report should have the following lines: • %AUTHMGR-5-FAIL: Authorization failed for client (001b.a912.3782) on Interface Gi0/3 AuditSessionID 0A000A760000008D4C69994E • %DOT1X_SWITCH-5-ERR_VLAN_NOT_FOUND: Attempt to assign non-existent or shutdown VLAN 666 to 802.1x port FastEthernet1/9 You can also run the troubleshooting workflow for the authentication. This workflow compares the ACL authentication log that contains RADIUS switch responses with the switch message database. Logging configuration (global) details may also be displayed: • Mandatory Expected Configuration Found On Device • logging monitor informational Missing • logging origin-id ip Missing • logging source-interface <*interface_id*> Missing • logging <*syslog_server_IP_address_x*> transport udp port 20514 Missing **Note** The network device must send syslog messages to the Monitoring ISE node server port 20514.
Possible Causes	The switch is missing (or contains the incorrect) name and numbers on the switch.
Resolution	Verify VLAN configuration(s) on the network access/enforcement points (switches) in your deployment.

Client Machine URL Redirection Function Not Working

Symptoms or Issue	Users are not appropriately redirected to the correct URL for authentication.
Conditions	The monitoring and troubleshooting configuration validator is designed to catch this. The web authentication configuration (global) details may display something like the following: • Mandatory Expected Configuration Found On Device • aaa authorization auth-proxy default group <*radius_group*> aaa authorization auth-proxy default group radius • aaa accounting auth-proxy default start-stop group <*radius_group*> Missing • ip admission name <*word*> proxy http inactivity-time 60 Missing fallback profile <*word*> • ip access-group <*word*> in • ip admission <*word*> Missing • ip http server ip http server • ip http secure-server ip http secure-server
Possible Causes	The switch is missing the **ip http server** and/or **ip http secure-server** command.
Resolution	Verify and (if necessary) adjust the configuration on the switch.

Cisco ISE Profiler is Not Able to Collect Data for Endpoints

Symptoms or Issue	Known devices on the network are not being profiled according to profiler policies in Cisco ISE.
Conditions	The monitoring and troubleshooting workflow catches device discovery configuration (global) details like the following: • Mandatory Expected Configuration Found On Device • ip dhcp snooping vlan <*Vlan_ID_for_DHCP_Snooping*> ip dhcp snooping vlan 1-4096 • no ip dhcp snooping information option Missing • ip dhcp snooping ip dhcp snooping • ip device tracking ip device tracking
Possible Causes	One or more Cisco ISE network enforcement points (switches) may be missing the **ip dhcp snooping** and/or **ip device tracking** commands that enable Profiler to perform its function.
Resolution	Verify switch configuration for those network segments where endpoints are not being appropriately profiled to ensure that: • The required information to profile the endpoint is being sent to Cisco ISE for it to profile. • Probes are configured on the network Policy Service ISE node entities.

RADIUS Accounting Packets (Attributes) Not Coming from Switch

Symptoms or Issue	The switch is not transmitting RADIUS accounting packets (attributes) to the RADIUS server.

Conditions	Click on the magnifying glass icon in Authentications to launch the authentication details. The session event section of the authentication report should show the accounting events. Clicking on the accounting events shows that audit-session-id fields are blank because the VSA[1] are blocked and no cisco-av-pair=audit-session-id messages are sent from the switch. The same can be done by running the accounting report for the day, where all audit-session-id fields should be blank. **Note** This issue is reported by the monitoring and troubleshooting configuration validator's RADIUS configuration (global) details. – Mandatory Expected Configuration Found On Device – radius-server attribute 6 support-multiple Missing – radius-server attribute 8 include-in-access-req radius-server attribute 8 include-in-access-req – radius-server host <*radius_ip_address1*> auth-port 1812 acct-port 1813 key <*radius_key*> Missing – radius-server vsa send accounting radius-server vsa send accounting – radius-server vsa send authentication radius-server vsa send authentication **Note** Be sure to include “radius-server attribute 25 access-request include” in the switch configuration.
Possible Causes	The Cisco ISE network enforcement device (switch) is missing the **radius-server vsa send accounting** command.
Resolution	Verify that the switch RADIUS configuration for this device is correct and features the appropriate command(s).

1. VSA = vendor-specific attribute

Policy Service ISE Node Not Passing Traffic

Symptoms or Issue	Network traffic is not traversing the network segment where a network policy enforcement device is installed.
Conditions	This issue can affect a Cisco ISE and other types of NADs that have been deployed as Policy Service ISE nodes to interoperate with another network device.
Possible Causes	There are multiple possible causes for an issue such as this.
Resolution	1. Use the **tcpdump** command in the NAD command-line interface (CLI) or from the Administration ISE node user interface at **Monitor > Troubleshoot > Diagnostic Tools > General Tools > TCP Dump** to verify whether the machine is receiving and forwarding traffic as required for your network. 2. If the TCP dump operation indicates that the Cisco ISE or NAD is working as configured, verify other adjacent network components.

Registered Nodes in Cisco ISE Managed List Following Standalone Reinstallation

Symptoms or Issue	The Administration ISE node user interface displays the Policy Service ISE node host name and configuration information when Cisco ISE is reimaged and installed as a new standalone node.
Conditions	This applies to a Cisco ISE node previously deployed as the Administration persona managing one or more associated Policy Service ISE nodes.
Possible Causes	If the Policy Service ISE nodes are still configured to send syslog updates to the Administration persona as it was originally set up, node information is learned when the Administration persona receives syslog messages. That information is likely used to populate the system summary page on the Administration persona.
Resolution	If you have not "deregistered" the Policy Service ISE nodes from the Cisco ISE node, reconfigure the Policy Service ISE nodes so that it sends syslog messages to itself, rather than the Cisco ISE node and restart the Policy Service ISE node. **Note** If you deregister any associated Policy Service ISE nodes before reinstalling the Cisco ISE software and reconfiguring the Administration persona, the Policy Service ISE nodes will operate in standalone mode and will not transmit the erroneous syslog updates.

Primary and Secondary Inline Posture Nodes Heartbeat Link Not Working

Symptoms or Issue	Two Inline Posture nodes that are deployed as high-availability peers appear dead to one another.
Conditions	Two Inline Posture nodes that are deployed in a "collocated" high-availability deployment.
Possible Causes	If the eth2 and eth3 interfaces on the Inline Posture nodes are not connected, both nodes will act as though the other node in the deployment has experienced some sort of failure.
Resolution	The heartbeat protocol requires a direct cable connection between the eth2 interfaces of both nodes in a high-availability pair, as well as a direct cable connection between the eth3 interfaces of the two nodes. You can use any Ethernet cable to make these connections.

Licensing and Administrator Access

- Certificate Expired, page 8

Certificate Expired

Symptoms or Issue	• Administrator begins to see alarm messages starting 30 days before certificate expiration. • If the certificate has expired, users cannot log into the network via Cisco ISE until the certificate has been refreshed.
Conditions	This issue can apply to any expired certificates on Cisco ISE.
Possible Causes	Your Cisco ISE certificate is about to expire or has expired.
Resolution	Refresh your Cisco ISE trusted certificate.

Configuration and Operation (Including High Availability)

- Client Machines Are Not Able to Authenticate, page 9
- Users Are Not Appropriately Redirected to URL, page 9
- Cannot Download Remote Client Provisioning Resources, page 10
- Lost Monitoring and Troubleshooting Data After Registering Policy Service ISE Node to Administration ISE Node, page 10
- Cisco ISE Monitoring Dashlets Not Visible with Internet Explorer 8, page 11

Client Machines Are Not Able to Authenticate

Symptoms or Issue	• Client sessions are not completing 802.1X authentication. • Click the magnifying glass icon in Authentications for the specific DACL to launch the authentication details. The content of the ACL should reveal one or more bad characters.
Conditions	Click on magnifying glass icon in Authentications to launch the Authentication Details. The session event section of the authentication report should have the following entry: `%EPM-4-POLICY_APP_FAILURE: IP 0.0.0.0| MAC 0002.b3e9.c926| AuditSessionID 0A000201000023903983718| AUTHTYPE DOT1X| POLICY_TYPE Named ACL| POLICY_NAME xACSACLx-IP-acl_access-4918c248| RESULT FAILURE| REASON Interface ACL not configured`
Possible Causes	• The DACL syntax may be incorrect or not configured in Cisco ISE. • When Cisco ISE enforces the DACL and there is no pre-authentication ACL configured on the switch, the NAD brings down the session and authentication fails.
Resolution	Depending on the nature of the problem: • Correct the DACL syntax configured in Cisco ISE and ensure that it also includes the **permit udp any any** command. • Configure the appropriate pre-authentication ACL on the switch.

Users Are Not Appropriately Redirected to URL

Symptoms or Issue	Administrator receives one or more “Bad URL” error messages from Cisco ISE.
Conditions	This scenario applies to 802.1X authentication as well as guest access sessions. Click the magnifying glass icon in Authentications to launch the Authentication Details. The authentication report should have the redirect URL in the RADIUS response section as well as the session event section (which displays the switch syslog messages).
Possible Causes	Redirection URL is entered incorrectly with invalid syntax or a missing path component.

Resolution	Verify that the redirection URL specified in Cisco ISE via Cisco-av pair "URL Redirect" is correct per the following options: • CWA Redirection URL: https://ip:8443/guestportal/gateway?sessionId=SessionIdValue&action=cwa • 802.1X Redirection URL: url-redirect=https://ip:8443/guestportal/gateway?sessionId=SessionIdValue&action=cpp

Cannot Download Remote Client Provisioning Resources

Symptoms or Issue	Administrator receives one or more "java.net.NoRouteToHostException: No route to host" error messages when trying to download client provisioning resources.
Conditions	This issue applies to any Cisco ISE that is connected to an external client provisioning resource store.
Possible Causes	Your internet connection may not be working properly or reliably.
Resolution	• Verify your internet connection settings. • Ensure that you have configured the correct proxy settings in Cisco ISE at **Administration > System > Settings > Proxy**.

Lost Monitoring and Troubleshooting Data After Registering Policy Service ISE Node to Administration ISE Node

Symptoms or Issue	The known collection of profiled endpoints is not visible on the secondary Policy Service ISE node when it is registered to the original (primary) Administration persona.
Conditions	This issue can come up in a deployment in which you register a new Policy Service ISE node to what has been, until the moment of registration, a standalone Cisco ISE node with a large store of known and profiled endpoints.
Possible Causes	Because of its potentially huge size, monitoring and troubleshooting data is not replicated between two nodes when the new node is registered to the original standalone Cisco ISE node. Cisco ISE does not replicate a data store that could conceivably be gigabytes in size, because it could impact network connectivity in a deployment environment.
Resolution	Ensure that you export monitoring and troubleshooting information *prior to* registering the new Policy Service ISE node to the formerly standalone Cisco ISE.

Cisco ISE Monitoring Dashlets Not Visible with Internet Explorer 8

Symptoms or Issue	Administrator sees one or more “There is a problem with this website's security certificate.” messages after clicking on the dashlets in the Cisco ISE monitoring portal.
Conditions	This issue is specific to Internet Explorer 8. (This issue has not been observed when using Mozilla Firefox.)
Possible Causes	The security certificate for the Internet Explorer 8 browser connection is invalid or expired.
Resolution	Use Internet Explorer 8 to reimport a valid security certificate to view the dashlets appropriately.

External Authentication Sources

- User Authentication Failed, page 12
- Missing User for RADIUS-Server Test Username in Cisco ISE Identities, page 12
- Connectivity Issues Between the Network Access Device (Switch) and Cisco ISE, page 13
- Active Directory Disconnected, page 13
- Cisco ISE Node Not Authenticating with Active Directory, page 14
- RADIUS Server Error Message Entries Appearing in Cisco ISE, page 14
- RADIUS Server Connectivity Issues (No Error Message Entries Appearing in Cisco ISE), page 15

User Authentication Failed

Symptoms or Issue	Authentications report failure reason: “Authentication failed: 22040 Wrong password or invalid shared secret”
Conditions	Click the magnifying glass icon in Authentications to view the steps in the authentication report that should display a brief series of messages as follows: • 24210 Looking up User in Internal Users IDStore - test-radius • 24212 Found User in Internal Users IDStore • 22040 Wrong password or invalid shared secret
Possible Causes	The user or device may not be supplying the correct credentials or RADIUS key to match with the external authentication source.
Resolution	Verify that the user credentials that are entered on the client machine are correct, and verify that the RADIUS server shared secret is correctly configured in both the NAD and Cisco ISE (they should be the same).

Missing User for RADIUS-Server Test Username in Cisco ISE Identities

Symptoms or Issue	The administrator notices one or more Authentications report failure messages like “Authentication failed: 22056 Subject not found in the applicable identity store(s)” for a given user ID.
Conditions	Click the magnifying glass icon in Authentications to view the messages in the Authentication Report. You should see a short series like the following: • 24210 Looking up User in Internal Users IDStore - test-radius • 24216 The user is not found in the internal users identity store • 22056 Subject not found in the applicable identity store(s)

Possible Causes	This message appears any time an authentication fails. In all cases, it's because the user is unknown to Cisco ISE. The subject could be a guest user who has not been added to the local database, a new employee who has not yet been appropriately provisioned in the network, or even a hacker. In addition, it is possible that the administrator did not configure the user ID in Cisco ISE.
Resolution	Check the local and external identity sources to verify whether the user ID exists, and if it does, ensure that both Cisco ISE and the associated access switch are configured to accept that user.

Connectivity Issues Between the Network Access Device (Switch) and Cisco ISE

Symptoms or Issue	Authentications report failure reason: “Authentication failed: 22040 Wrong password or invalid shared secret”
Conditions	Click the magnifying glass icon in Authentications to display authentication report entries like the following: • 24210 Looking up User in Internal Users IDStore - test-radius • 24212 Found User in Internal Users IDStore • 22040 Wrong password or invalid shared secret
Possible Causes	The network administrator may not have specified the correct password to enable the switch (or other NAD) to authenticate with Cisco ISE.
Resolution	Verify that the password that is configured on the NAD is correct to authenticate with Cisco ISE.

Active Directory Disconnected

Symptoms or Issue	The connection between Cisco ISE and the Active Directory server has been terminated, resulting in user authenticating failure.
Conditions	This issue is pertinent to any Active Directory domain topology that is connected to Cisco ISE.
Possible Causes	This scenario is most commonly caused by clock drift due to not syncing time via NTP[1] on VMware. This issue can also arise if the Cisco ISE FQDN[2] changes and/or the name of the certificate imported on the client machine has changed.
Resolution	Ensure that your Active Directory domain and Cisco ISE are aligned to the same NTP server source. Shut down or pause your Active Directory server and try to authenticate an employee to the network.

1. NTP = Network Time Protocol
2. FQDN = fully-qualified domain name

Cisco ISE Node Not Authenticating with Active Directory

Symptoms or Issue	The administrator receives “authentication failure” messages in the Authentication Failure Report on the Administration ISE node.
Conditions	This issue applies to Cisco ISE policy enforcement nodes added to an existing AD domain.
Possible Causes	• The administrator may not have changed the AD password on after joining the Cisco ISE node to the AD domain. • The account used to join Cisco ISE to the Active Directory domain may have an expired password.
Resolution	Change the account password that was used to join the AD domain after adding Cisco ISE to Active Directory.

RADIUS Server Error Message Entries Appearing in Cisco ISE

Symptoms or Issue	• Unsuccessful RADIUS or AAA[1] functions on Cisco ISE • Error messages in the **Monitor > Authentication** event entries
Conditions	This scenario can become an issue in a system where Cisco ISE is configured to perform user authentication via an external identity source on the network.
Possible Causes	The following are possible causes for losing connectivity with the external identity source: • Subject not found in the applicable identity source • Wrong password or invalid shared secret • Could not locate network device or AAA client

Resolution	Check the Cisco ISE dashboard (**Monitor > Authentications**) for any indication regarding the nature of RADIUS communication loss. (Look for instances of your specified RADIUS usernames and scan the system messages that are associated with any error message entries.) Log into the Cisco ISE CLI[2] and enter the following command to produce RADIUS attribute output that may aid in debugging connection issues: **test aaa group radius** <*username*> <*password*> **new-code** If this test command is successful, you should see the following attributes: • Connect port • Connect NAD IP address • Connect Policy Service ISE node IP address • Correct server key • Recognized username or password • Connectivity between the NAD and Policy Service ISE node You can also use this command to help narrow the focus of the potential problem with RADIUS communication by deliberately specifying incorrect parameter values in the command line and then returning to the administrator dashboard (**Monitor > Authentications**) to view the type and frequency of error message entries that result from the incorrect command line. For example, to test whether or not user credentials may be the source of the problem, enter a username and or password that you *know* is incorrect, and then go look for error message entries that are pertinent to that username in the **Monitor > Authentications** page to see what Cisco ISE is reporting.) **Note** This command does not validate whether or not the NAD is configured to use RADIUS, nor does it verify whether the NAD is configured to use the new AAA model.

1. AAA = authentication, authorization, and accounting
2. CLI = command-line interface

RADIUS Server Connectivity Issues (No Error Message Entries Appearing in Cisco ISE)

Symptoms or Issue	• Unsuccessful RADIUS or AAA functions in Cisco ISE • The NAD is unable to ping the Policy Service ISE node
Conditions	This scenario is applicable in a system in which Cisco ISE is configured to perform user authentication via an external RADIUS server on the network.
Possible Causes	The following are possible causes for losing connectivity with the RADIUS server: • Network connectivity issue or issues • Bad server IP address • Bad server port

Resolution	If you are unable to ping the Policy Service ISE node from the NAD, try any or all of these possible solutions: • Verify the NAD IP address • Try using Traceroute and other appropriate "sniffer"-type tools to isolate the source of disconnection. (In a production environment, be cautious of overusing debug functions, because they commonly consume large amounts of available bandwidth and CPU, which can impact normal network operation.) Check the Cisco ISE "TCP Dump" report for the given Policy Service ISE node to see if there are any indications.

Client Access, Authentication, and Authorization

- Debug Logging for Cisco ISE Agents, page 17
- Cannot Authenticate on Profiled Endpoint, page 19
- Quarantined Endpoints Do Not Renew Authentication Following Policy Change, page 20
- Endpoint Does Not Align to the Expected Profile, page 21
- User is Unable to Authenticate Against the Local Cisco ISE Identity Store, page 21
- Certificate-Based User Authentication via Supplicant Failing, page 22
- 802.1X Authentication Fails, page 23
- Users Are Reporting Unexpected Network Access Issues, page 23
- Authorization Policy Not Working, page 24
- Switch is Dropping Active AAA Sessions, page 25
- URL Redirection on Client Machine Fails, page 26
- Agent Download Issues on Client Machine, page 28
- Agent Login Dialog Not Appearing, page 29
- Agent Fails to Initiate Posture Assessment, page 29
- Agent Displays “Temporary Access”, page 30
- Cisco ISE Does Not Issue CoA Following Authentication, page 30

Debug Logging for Cisco ISE Agents

For any of the above issues pertaining to the Cisco NAC Agent, Cisco NAC Web Agent, or Mac OS X Agent, you may find it useful to extract and have Agent debug logs at your disposal to aid any troubleshooting efforts.

This section describes how to view and/or enable debug logging for agents available in Cisco ISE. Refer to the following sections for steps for each Agent type:

- Generate Cisco NAC Agent Debug Logs
- Cisco NAC Web Agent Logs
- Generate Mac OS X Agent Debug Log

Copy these event logs to include them in a customer support case.

Generate Cisco NAC Agent Debug Logs

To generate Cisco NAC Agent logs using the Cisco Log Packager utility, refer to the “Create Agent Log Files Using the Cisco Log Packager” section of the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(2)*.

Cisco NAC Web Agent Logs

The Cisco NAC Web Agent can generate logs when downloaded and executed. By default, the Cisco NAC Web Agent writes the log file upon startup with debugging turned on. The Cisco NAC Web Agent generates the following log files for troubleshooting purposes: **webagent.log** and **webagentsetup.log**. These files should be included in any TAC support case for the Web Agent. Typically, these files are located in the user's temp directory, in the form:

C:\Document and Settings\<*user*>\Local Settings\Temp\webagent.log

C:\Document and Settings\<*user*>\Local Settings\Temp\webagentsetup.log

If these files are not visible, check the TEMP environment variable setting. From a command-prompt, type "echo %TEMP%" or "cd %TEMP%".

When the client uses Microsoft Internet Explorer, the Cisco NAC Web Agent is downloaded to the **C:\Documents and Settings\<*user*>\Local Settings\Temporary internet files** directory.

Generate Mac OS X Agent Debug Log

For Mac OS X Agents, the Agent **event.log** file and **preference.plist** user preferences file are available under <*username*> **> Library > Application Support > Cisco Systems > CCAAgent.app**. To change or specify the LogLevel setting, however, you must access the global **setting.plist** file (which is *different* from the user-level **preference.plist** file).

Because Cisco does not recommend allowing individual users to change the LogLevel value on the client machine, you must be a superuser or root user to alter the global **setting.plist** system preferences file and specify a different Agent LogLevel.

To view and/or change the Agent LogLevel:

Step 1 Open the navigator pane and navigate to <*local drive ID*> **> Applications**.

Step 2 Highlight and right-click the **CCAAgent.app** icon to bring up the selection menu.

Step 3 Choose **Show Package Contents > Resources**.

Step 4 Choose **setting.plist**.

Step 5 If you want to change the current LogLevel setting using Mac **Property Editor**, find the current LogLevel Key and replace the exiting value with one of the following:

- **Info**—Include only informational messages in the event log
- **Warn**—Include informational and warning messages in the event log
- **Error**—Include informational, warning, and error messages in the event log
- **Debug**—Include all Agent messages (including informational, warning, and error) in the event log

Note The **Info** and **Warn** entry types only feature a few messages pertaining to very specific Agent events. Therefore, you will probably only need either the **Error** or **Debug** Agent event log level when troubleshooting Agent connection issues.

Note If the .plist file is not editable (displayed as binary characters), you either need to use the Mac **Property List Editor** utility from the Mac OS X CD-ROM or acquire another similar tool to edit the **setting.plist** file.

Property List Editor is an application included in the Apple Developer Tools for editing .plist files. You can find it at <*CD-ROM*>/Developer/Applications/Utilities/Property List Editor.app.

If the **setting.plist** file *is* editable, you can use a standard text editor like vi to edit the LogLevel value in the file.

You must be the root user to edit the file.

Cannot Authenticate on Profiled Endpoint

Symptoms or Issue	• The IP phone was profiled but was not authorized properly. Therefore, it was not assigned to the voice VLAN. • The IP phone was profiled and authorized properly, but was not assigned to the correct voice VLAN. • The endpoint has been successfully profiled in Cisco ISE, but user authentication fails.
Conditions	The administrator will see the Authentications Log Error message: "22056 Subject not found in the applicable identity store(s)" containing the following entries: • 24210 Looking up User in Internal Users IDStore - 00:03:E3:2A:21:4A • 24216 The user is not found in the internal users identity store • 22056 Subject not found in the applicable identity store(s)
Possible Causes	• This could be either a MAB[1] or 802.1X authentication issue. • The authorization profile could be missing the Cisco av-pair="device-traffic-class=voice" attribute. As a result, the switch does not recognize the traffic on the voice VLAN. • The administrator did not add the endpoint as static identity, or did not allow an unregistered endpoint to pass (create a policy rule to "Continue/Continue/Continue" upon failure).

Resolution	• Verify that the Authorization Policy is framed properly for groups and conditions, and check to see whether the IP phone is profiled as an "IP phone" or as a "Cisco-device." • Verify the switch port configuration for multidomain and voice VLAN configuration. • Add the continue/continue/continue to allow the endpoint to pass: **a.** Choose **Policy > Policy Elements > Configurations** and choose **Allowed Protocol Service**s to create a Protocol Policy. MAC authentications use PAP[2]/ASCII and EAP-MD5[3] protocols. Enable the following MAB_Protocols settings: – Process Host Lookup – PAP/ASCII – Detect PAP as Host Lookup – EAP-MD5 – Detect EAP-MD5 as Host Lookup **b.** From the main menu, choose **Policy > Authentication**. **c.** Change the authentication method from Simple to Rule-Based **d.** Use the action icon to create new Authentication Method entries for MAB: – Name: MAB – Condition: IF MAB RADIUS:Service-Type == Call Check – Protocols: allow protocols MAB_Protocols and use – Identity Source: Internal – Hosts: Continue/Continue/Continue

1. MAB = MAC authentication bypass
2. PAP = Password Authentication Protocol
3. EAP = Extensible AUthentication Protocol; MD5 = Message Digest 5

Quarantined Endpoints Do Not Renew Authentication Following Policy Change

Symptoms or Issue	Authentication has failed following policy change or additional identity and no reauthentication is taking place. The endpoint in question remains unable to connect or authentication fails.
Conditions	This issue often occurs on client machines that are failing posture assessment per the posture policy that is assigned to the user role.
Possible Causes	The authentication timer may not be set correctly on the client machine, or the authentication interval may not be set correctly on the switch.

Resolution	There are several possible resolutions for this issue: 1. Check the Session Status Summary report in Cisco ISE for the specified NAD or switch, and ensure that the interface has the appropriate authentication interval configured. 2. Enter "show running configuration" on the NAD/switch and ensure that the interface is configured with an appropriate "authentication timer restart" setting. (For example, "authentication timer restart 15," and "authentication timer reauthenticate 15.") 3. Try entering "interface shutdown" and "no shutdown" to bounce the port on the NAD/switch and force reauthentication following a potential configuration change in Cisco ISE.

Note Since CoA requires a MAC address or session ID, Cisco recommends that you do not bounce the port that is shown in the Network Device SNMP report.

Endpoint Does Not Align to the Expected Profile

Symptoms or Issue	An IP phone is plugged in and the profile appears as a "Cisco-Device."
Conditions	Launch the Endpoint Profiler/Endpoint Profiler Summary report and click **Details** for the MAC address that corresponds to the profiled endpoint in question.
Possible Causes	• There could be an SNMP configuration issue on Cisco ISE, the switch, or both. • The profile is likely not configured correctly, or contains the MAC address of the endpoint already.
Resolution	• Verify the SNMP version configuration on both Cisco ISE and the switch for SNMP trap and SNMP server settings. • The Profiler profile needs to be updated. Choose **Policy > Profiling > Profiling Policies** in Cisco ISE and manually map this endpoint to that profile.

User is Unable to Authenticate Against the Local Cisco ISE Identity Store

Symptoms or Issue	User cannot authenticate from supplicant.
Conditions	Authentications report failure reason: "Authentication failed: 22056 Subject not found in the applicable identity store(s)" Click the magnifying glass in Authentications to launch the Authentication report that displays the following: • 24210 Looking up User in Internal Users IDStore - ACSXP-SUPP2\Administrator • 24216 The user is not found in the internal users identity store

Possible Causes	The supplicant is providing a name and password to authenticate against the local Cisco ISE user database, but those credentials are not configured in the local database.
Resolution	Verify that the user credentials are configured in the Cisco ISE local identity store.

Certificate-Based User Authentication via Supplicant Failing

Symptoms or Issue	User authentication is failing on the client machine, and the user is receiving a "RADIUS Access-Reject" form of message.
Conditions	(This issue occurs with authentication protocols that require certificate validation.) Possible Authentications report failure reasons: • "Authentication failed: 11514 Unexpectedly received empty TLS message; treating as a rejection by the client" • "Authentication failed: 12153 EAP-FAST failed SSL/TLS handshake because the client rejected the Cisco ISE local-certificate" Click the magnifying glass icon from Authentications to display the following output in the Authentication Report: • 12305 Prepared EAP-Request with another PEAP challenge • 11006 Returned RADIUS Access-Challenge • 11001 Received RADIUS Access-Request • 11018 RADIUS is re-using an existing session • 12304 Extracted EAP-Response containing PEAP challenge-response • 11514 Unexpectedly received empty TLS message; treating as a rejection by the client • 12512 Treat the unexpected TLS acknowledge message as a rejection from the client • 11504 Prepared EAP-Failure • 11003 Returned RADIUS Access-Reject • 11006 Returned RADIUS Access-Challenge • 11001 Received RADIUS Access-Request • 11018 RADIUS is re-using an existing session • 12104 Extracted EAP-Response containing EAP-FAST challenge-response • 12815 Extracted TLS Alert message • 12153 EAP-FAST failed SSL/TLS handshake because the client rejected the Cisco ISE local-certificate • 11504 Prepared EAP-Failure • 11003 Returned RADIUS Access-Reject **Note** This is an indication that the client does not have or does not trust the Cisco ISE certificates.

Possible Causes	The supplicant or client machine is not accepting the certificate from Cisco ISE. The client machine is configured to validate the server certificate, but is not configured to trust the Cisco ISE certificate.
Resolution	The client machine must accept the Cisco ISE certificate to enable authentication.

802.1X Authentication Fails

Symptoms or Issue	The user logging in via the client machine sees an error message from the supplicant that indicates that 802.1X authentication has failed.
Conditions	Troubleshooting Steps: 1. Choose **Monitor > Authentications**. 2. Scroll over and look for the "Failure reason."
Possible Causes	Look for the details of the failed authentication record and click on the failure reason link under **Details > Resolution for the Authentication**. The failure reason should be listed.
Resolution	Correct the failure reason per the findings that are defined in the Possible Causes.

Note If authentication fails and there are no Authentications entries to search (assuming monitoring and troubleshooting is running properly), complete the following steps:

1. Ensure that the RADIUS server configuration on the switch is pointing to Cisco ISE.
2. Check network connectivity between the switch and Cisco ISE.
3. Verify that the Policy Service ISE node is running on Cisco ISE to ensure that it can receive RADIUS requests.

Users Are Reporting Unexpected Network Access Issues

Symptoms or Issue	Several symptoms for this issue could be taking place, including the following: • Users are being asked to download an agent other than what they expect. • Users who should have full network access are only allowed limited network access. • Although users are passing posture assessment, they are not getting the appropriate level of network access. • Users who should be allowed into the corporate (Access) VLAN are being left in the Authentication VLAN following authentication.
Conditions	Users are successfully authenticated, but are unable to get network access.

Possible Causes	• The administrator may not have specified the correct authorization profile. • The administrator did not define the appropriate policy conditions for the user access level. • The authorization profile, itself, might not have been framed properly.
Resolution	Ensure that the Identity Group Conditions are defined appropriately to support the authorization profile that is required for the user groups in question. 1. Choose **Monitor > Authentication**. 2. Look for the identity group to which the user belongs. 3. Look at the authorization profile that is selected for that identity group. 4. Choose **Policy > Authorization** and verify that the correct rule is matching for that identity group. 5. If not, debug for the reason why the correct authorization policy is not matching.

Authorization Policy Not Working

Symptoms or Issue	The authorization policy that is specified by the administrator is the correct one, but the endpoint is not receiving the configured VLAN IP.
Conditions	This issue applies to standard user authorization sessions in a wired environment.
Possible Causes	The preauthorization ACL could be blocking DHCP traffic.

Resolution	• Ensure that the Cisco IOS release on the switch is equal to or more recent than the Cisco IOS Release 12.2.(53)SE.
	• Ensure that the identity group conditions are defined appropriately.
	• Check for the client machine port VLAN by using **show vlan** on the access switch. If the port is not showing the correct authorization profile VLAN, ensure that VLAN enforcement is appropriate to reach out to the DHCP server. If the VLAN is correct, the preauthorization ACL could be blocking DHCP traffic. Ensure that the preauthorization DACL is as follows:
	`remark Allow DHCP`
	`permit udp any eq bootpc any eq bootps`
	`remark Allow DNS`
	`permit udp any any eq domain`
	`remark ping`
	`permit icmp any any`
	`permit tcp any host 80.0.80.2 eq 443 --> This is for URL redirect`
	`permit tcp any host 80.0.80.2 eq www`
	`permit tcp any host 80.0.80.2 eq 8443 --> This is for guest portal port`
	`permit tcp any host 80.0.80.2 eq 8905 --> This is for posture communication between NAC agent and ISE (Swiss ports)`
	`permit udp any host 80.0.80.2 eq 8905 --> This is for posture communication between NAC agent and ISE (Swiss ports)`
	`permit udp any host 80.0.80.2 eq 8906 --> This is for posture communication between NAC agent and ISE (Swiss ports)`
	`deny ip any any`
	• Ensure the session is created on the switch by entering **show epm session summary**. If the IP address of the session shown is "not available," ensure that the following configuration lines appear on the switch:
	`ip dhcp snooping vlan 30-100`
	`ip device tracking`

Switch is Dropping Active AAA Sessions

Symptoms or Issue	802.1X and MAB authentication and authorization are successful, but the switch is dropping active sessions and the **epm session summary** command does not display any active sessions.
Conditions	This applies to user sessions that have logged in successfully and are then being terminated by the switch.
Possible Causes	• The preauthentication ACL (and the subsequent DACL enforcement from Cisco ISE) on the NAD may not be configured correctly for that session. • The preauthentication ACL is configured and the DACL is downloaded from Cisco ISE, but the switch brings the session down. • Cisco ISE may be enforcing a preposture VLAN assignment rather than the (correct) postposture VLAN, which can also bring down the session.

Resolution	• Ensure the Cisco IOS release on the switch is equal to or more recent than Cisco IOS Release 12.2.(53)SE.
	• Check to see whether or not the DACL name in Cisco ISE contains a blank space (possibly around or near a hyphen "-"). There should be no space in the DACL name. Then ensure that the DACL syntax is correct and that it contains no extra spaces.
	• Ensure that the following configuration exists on the switch to interpret the DACL properly (if not enabled, the switch may terminate the session):
	`radius-server attribute 6 on-for-login-auth`
	`radius-server attribute 8 include-in-access-req`
	`radius-server attribute 25 access-request include`
	`radius-server vsa send accounting`
	`radius-server vsa send authentication`

URL Redirection on Client Machine Fails

Symptoms or Issue	The URL redirection page in the client machine's browser does not correctly guide the end user to the appropriate URL.
Conditions	This issue is most applicable to 802.1X authentication sessions that require URL redirection and Guest Centralized Web Authentication (CWA) login sessions.
Possible Causes	(There are multiple causes for this issue. See the **Resolutions** descriptions that follow for explanation.)

Resolution

- The two Cisco av-pairs that are configured on the authorization profile should exactly match the example below. (Note: Do *not* replace the "IP" with the actual Cisco ISE IP address.)
  - url-redirect=https://ip:8443/guestportal/gateway?...lue&action=cpp
  - url-redirect-acl=ACL-WEBAUTH-REDIRECT (ensure that this ACL is also defined on the access switch)
- Ensure that the URL redirection portion of the ACL have been applied to the session by entering the **show epm session ip** <*session IP*> command on the switch. (Where the session IP is the IP address that is passed to the client machine by the DHCP server.)

```
Admission feature : DOT1X
AAA Policies : #ACSACL#-IP-Limitedaccess-4cb2976e
URL Redirect ACL : ACL-WEBAUTH-REDIRECT
URL Redirect :
https://node250.cisco.com:8443/guestportal/gateway?sessionId=0A000A72
0000A45A2444BFC2&action=cpp
```

- Ensure that the preposture assessment DACL that is enforced from the Cisco ISE authorization profile contains the following command lines:

```
remark Allow DHCP
permit udp any eq bootpc any eq bootps
remark Allow DNS
permit udp any any eq domain
remark ping
permit icmp any any
permit tcp any host 80.0.80.2 eq 443 --> This is for URL redirect
permit tcp any host 80.0.80.2 eq www --> Provides access to internet
permit tcp any host 80.0.80.2 eq 8443 --> This is for guest portal
port
permit tcp any host 80.0.80.2 eq 8905 --> This is for posture
communication between NAC agent and ISE (Swiss ports)
permit udp any host 80.0.80.2 eq 8905 --> This is for posture
communication between NAC agent and ISE (Swiss ports)
permit udp any host 80.0.80.2 eq 8906 --> This is for posture
communication between NAC agent and ISE (Swiss ports)
deny ip any any
```

Note Ensure that the above URL Redirect has the proper Cisco ISE FQDN.

Resolution (continued)	• Ensure that the ACL with the name "ACL-WEBAUTH_REDIRECT" exists on the switch as follows:
	`ip access-list extended ACL-WEBAUTH-REDIRECT`
	`deny ip any host 80.0.80.2`
	`permit ip any any`
	• Ensure that the http and https servers are running on the switch:
	`ip http server`
	`ip http secure-server`
	• Ensure that, if the client machine employs any kind of personal firewall, it is disabled.
	• Ensure that the client machine browser is not configured to use any proxies.
	• Verify connectivity between the client machine and the Cisco ISE IP address.
	• If Cisco ISE is deployed in a distributed environment, make sure that the client machines are aware of the Policy Service ISE node FQDN.
	• Ensure that the Cisco ISE FQDN is resolved and reachable from the client machine.

Agent Download Issues on Client Machine

Symptoms or Issue	Client machine browser displays a "no policy matched" error message after user authentication and authorization.
Conditions	This issue applies to user sessions during the client provisioning phase of authentication.
Possible Causes	The client provisioning resource policy could be missing required settings.
Resolution	• Ensure that a client provisioning policy exists in Cisco ISE. If yes, verify the policy identity group, conditions, and type of agent(s) defined in the policy. (Also ensure whether or not there is any agent profile configured under **Policy > Policy Elements > Results > Client Provisioning > Resources > Add > ISE Posture Agent Profile**, even a profile with all default values.) • Try reauthenticating the client machine by bouncing the port on the access switch.

Note Remember that the client provisioning agent installer download requires the following:

- The user must allow the ActiveX installer in the browser session the first time an agent is installed on the client machine. (The client provisioning download page prompts for this.)
- The client machine must have Internet access.

Agent Login Dialog Not Appearing

Symptoms or Issue	The agent login dialog box does not appear to the user following client provisioning.
Conditions	This issue can generally take place during the posture assessment phase of any user authentication session.
Possible Causes	There are multiple possible causes for this type of issue. See the following **Resolution** descriptions for details.

Resolution	• Ensure that the agent is running on the client machine.
	• Ensure that the Cisco IOS release on the switch is equal to or more recent than Cisco IOS Release 12.2.(53)SE.
	• Ensure that the discovery host address on the Cisco NAC agent or Mac OS X agent is pointing to the Cisco ISE FQDN. (Right-click on the NAC agent icon, choose **Properties**, and check the discovery host.)
	• Ensure that the access switch allows Swiss communication between Cisco ISE and the end client machine. Limited access ACL applied for the session should allow Swiss ports:
	`remark Allow DHCP`
	`permit udp any eq bootpc any eq bootps`
	`remark Allow DNS`
	`permit udp any any eq domain`
	`remark ping`
	`permit icmp any any`
	`permit tcp any host 80.0.80.2 eq 443 --> This is for URL redirect`
	`permit tcp any host 80.0.80.2 eq www --> Provides access to internet`
	`permit tcp any host 80.0.80.2 eq 8443 --> This is for guest portal port`
	`permit tcp any host 80.0.80.2 eq 8905 --> This is for posture communication between NAC agent and ISE (Swiss ports)`
	`permit udp any host 80.0.80.2 eq 8905 --> This is for posture communication between NAC agent and ISE (Swiss ports)`
	`deny ip any any`
	• If the agent login dialog still does not appear, it could be a certificate issue. Ensure that the certificate that is used for Swiss communication on the end client is in the Cisco ISE certificate trusted list.
	• Ensure that the default gateway is reachable from the client machine.

Agent Fails to Initiate Posture Assessment

Symptoms or Issue	The user is presented with a “Clean access server not available” message.
Conditions	This issue applies to any agent authentication session from Cisco ISE.
Possible Causes	This error could mean that either the session has terminated or Cisco ISE is no longer reachable on the network.

Resolution	• The user can try to ping the default gateway or the RADIUS server IP address or FQDN supplied by the network administrator. • The user can try to log into the network again. • The administrator can check network access attributes for the user (like the assigned VLAN, ACLs, routing, execute the **nslookup** command on the client, client machine DNS connection, etc.).

Agent Displays "Temporary Access"

Symptoms or Issue	A client machine is granted "Temporary Access" following login and authentication, but administrator and user expect full network access.
Conditions	This issue is applicable to any client machine login session using an agent to connect.
Possible Causes	If the NAC Agent is running on the client and: • The interface on the client machine goes down • The session is terminated
Resolution	The user must try to verify network connectivity and then try to log in again (and pass through posture assessment, as well) to attempt to re-establish the connection.

Cisco ISE Does Not Issue CoA Following Authentication

Symptoms or Issue	CoA is not issued following client machine login and authentication.
Conditions	This specific issue is only applicable in a wired environment where CoA is required on the client machine to complete authentication.
Possible Causes	The access switch may not have the required configuration to support CoA for the client machine.

Resolution	• Ensure that the Cisco IOS release on the switch is equal to or more recent than Cisco IOS Release 12.2.(53)SE.
	• Ensure that the switch configuration features the following commands necessary to enable CoA:
	`aaa server radius dynamic-author`
	`client 80.0.80.2 server-key cisco456 --> ISE ip.`
	`server-key cisco456`

Error Messages

- ACTIVE_DIRECTORY_USER_INVALID_CREDENTIALS, page 31
- ACTIVE_DIRECTORY_USER_AUTH_FAILED, page 31
- ACTIVE_DIRECTORY_USER_PASSWORD_EXPIRED, page 32
- ACTIVE_DIRECTORY_USER_WRONG_PASSWORD, page 32
- ACTIVE_DIRECTORY_USER_ACCOUNT_DISABLED, page 32
- ACTIVE_DIRECTORY_USER_RESTRICTED_LOGON_HOURS, page 32
- ACTIVE_DIRECTORY_USER_NON_COMPLIANT_PASSWORD, page 32
- ACTIVE_DIRECTORY_USER_UNKNOWN_DOMAIN, page 33
- ACTIVE_DIRECTORY_USER_ACCOUNT_EXPIRED, page 33
- ACTIVE_DIRECTORY_USER_ACCOUNT_LOCKED_OUT, page 33
- ACTIVE_DIRECTORY_GROUP_RETRIEVAL_FAILED, page 33
- ACTIVE_DIRECTORY_MACHINE_AUTHENTICATION_DISABLED, page 33
- ACTIVE_DIRECTORY_ATTRIBUTE_RETRIEVAL_FAILED, page 34
- ACTIVE_DIRECTORY_PASSWORD_CHANGE_DISABLED, page 34
- ACTIVE_DIRECTORY_USER_UNKNOWN, page 34
- ACTIVE_DIRECTORY_CONNECTION_FAILED, page 34
- ACTIVE_DIRECTORY_BAD_PARAMETER, page 34
- ACTIVE_DIRECTORY_TIMEOUT, page 35

ACTIVE_DIRECTORY_USER_INVALID_CREDENTIALS

Description	This Authentication Failure message indicates that the user's credentials are invalid.
Resolution	Check if the Active Directory user account and credentials that are used to connect to the Active Directory domain are correct.

ACTIVE_DIRECTORY_USER_AUTH_FAILED

Description	This Authentication Failure message indicates that the user authentication has failed. You will see this message when the user or machine password is not found in Active Directory.
Resolution	Check if the Active Directory user account and credentials that are used to connect to the Active Directory domain are correct.

ACTIVE_DIRECTORY_USER_PASSWORD_EXPIRED

Description	This Authentication Failure message appears when the user's password has expired.
Resolution	If the Active Directory user account is valid, then reset the account in Active Directory. If the user account has expired, but if it is still needed, then renew it. If the user account has expired and is no longer valid, investigate the reasons for the attempts.

ACTIVE_DIRECTORY_USER_WRONG_PASSWORD

Description	This Authentication Failure message appears when the user has entered an incorrect password.
Resolution	Check if the Active Directory user account and credentials that are used to connect to the Active Directory domain are correct.

ACTIVE_DIRECTORY_USER_ACCOUNT_DISABLED

Description	This Authentication Failure message appears when the user account is disabled in Active Directory.
Resolution	If the Active Directory user account is valid, then reset the account in Active Directory. If the user account has expired, but if it is still needed, then renew it. If the user account has expired and is no longer valid, investigate the reasons for the attempts.

ACTIVE_DIRECTORY_USER_RESTRICTED_LOGON_HOURS

Description	This Authentication Failure message appears when the user logs in during restricted hours.
Resolution	If the user access is valid, then update the user access policy in Active Directory. If the user access is invalid (restricted at this time), then investigate the reasons for the attempts.

ACTIVE_DIRECTORY_USER_NON_COMPLIANT_PASSWORD

Description	This Authentication Failure message appears if the user has a password that is not compliant with the password policy.
Resolution	Reset the password in Active Directory such that it is compliant with the password policy in Active Directory.

ACTIVE_DIRECTORY_USER_UNKNOWN_DOMAIN

Description	This Authentication Failure message appears if Active Directory is unable to locate the specified domain.
Resolution	Check the configuration of Active Directory in the Administration ISE node user interface and the DNS[1] configuration in the Cisco ISE CLI.

1. DNS = domain name service

ACTIVE_DIRECTORY_USER_ACCOUNT_EXPIRED

Description	This message appears when the user account in Active Directory has expired.
Resolution	If the user account has expired, but is still needed, then renew the user account. If the user account has expired and is no longer valid, investigate the reasons for the attempts.

ACTIVE_DIRECTORY_USER_ACCOUNT_LOCKED_OUT

Description	This Authentication Failure message appears if the user account has been locked out.
Resolution	If the user attempts to log in with correct credentials, reset the user's password. Otherwise, investigate the attempts that caused the lock out.

ACTIVE_DIRECTORY_GROUP_RETRIEVAL_FAILED

Description	This Authentication Failure message appears if Active Directory is unable to retrieve the groups.
Resolution	Check if the Active Directory configuration in the Administration ISE node user interface is correct.

ACTIVE_DIRECTORY_MACHINE_AUTHENTICATION_DISABLED

Description	This Authentication Failure message appears if machine authentication is not enabled in Active Directory.
Resolution	Enable Machine Authentication in Active Directory, if required.

ACTIVE_DIRECTORY_ATTRIBUTE_RETRIEVAL_FAILED

Description	This Authentication Failure message appears if Active Directory is unable to retrieve the attributes that you have specified.
Resolution	Check if the Active Directory configuration in the Administration ISE node user interface is correct.

ACTIVE_DIRECTORY_PASSWORD_CHANGE_DISABLED

Description	This Authentication Failure message appears if the password change option is disabled in Active Directory.
Resolution	Enable Password Change in Active Directory, if required.

ACTIVE_DIRECTORY_USER_UNKNOWN

Description	This Invalid User message appears if the user information is not found in Active Directory.
Resolution	Check for the origin of the invalid attempts. If it is from a valid user, ensure that the user account is configured correctly in Active Directory.

ACTIVE_DIRECTORY_CONNECTION_FAILED

Description	This External Error message appears when Cisco ISE is unable to establish a connection with Active Directory.
Resolution	Check if the Active Directory configuration in the Administration ISE node user interface is correct.

ACTIVE_DIRECTORY_BAD_PARAMETER

Description	This External Error message appears when you have provided an invalid input.
Resolution	Check if the Active Directory configuration in the Administration ISE node user interface is correct.

ACTIVE_DIRECTORY_TIMEOUT

Description	This External Error message appears when a timeout event has occurred.
Resolution	Check if the Active Directory configuration in the Administration ISE node user interface is correct

Configure NADs for ISE Monitoring

To help troubleshoot failures with endpoint authentication and authorization, network access devices (NADs) can be configured to send syslog messages to the ISE Monitoring node. The logs can be correlated to authentication and authorization events and will be displayed in the details of the RADIUS authentication logs.

Note Sending syslog from NADs to ISE should be used for troubleshooting purposes only as this additional logging increases the load on the Monitoring node. Logging should only be enabled on specific NADs where endpoint is connected and should be disabled when the troubleshooting session is completed. If possible, it is recommended to filter the logs sent to ISE to those listed in Syslog Messages Collected, page 35.

To enable a switch in your network to send syslog messages for ISE troubleshooting purposes, use the following commands.

```
epm logging
logging monitor informational
logging origin-id ip
logging source-interface <interface_id>
logging host <syslog_server_IP_address_x> transport udp port 20514
```

Note The origin-id ip address should be set to match source-interface IP address. The interface_id is the interface that will send syslog messages. Syslog messages will be sourced from the IP address configured for this interface. The syslog_server_IP_address should be the Primary MnT node.

Syslog Messages Collected

The following NAD syslog messages are collected:

AP-6-AUTH_PROXY_AUDIT_START

AP-6-AUTH_PROXY_AUDIT_STOP

AP-1-AUTH_PROXY_DOS_ATTACK

AP-1-AUTH_PROXY_RETRIES_EXCEEDED

AP-1-AUTH_PROXY_FALLBACK_REQ

AP-1-AUTH_PROXY_AAA_DOWN

AUTHMGR-5-MACMOVE

AUTHMGR-5-MACREPLACE

AUTHMGR-5-START/SUCCESS/FAIL

AUTHMGR-SP-5-VLANASSIGN/VLANASSIGNERR

DOT1X-5-SUCCESS/FAIL

DOT1X_SWITCH-5-ERR_VLAN_NOT_FOUND

EPM-6-POLICY_REQ

EPM-6-POLICY_APP_SUCCESS/FAILURE

EPM-6-IPEVENT:

MAB-5-SUCCESS/FAIL

MKA-5-SESSION_START

MKA-5-SESSION_STOP

MKA-5-SESSION_REAUTH

MKA-5-SESSION_UNSECURED

MKA-5-SESSION_SECURED

MKA-5-KEEPALIVE_TIMEOUT

RADIUS-4-RADIUS_DEAD

Troubleshooting APIs

You can use the following troubleshooting APIs to query information from Cisco ISE that could aid in general troubleshooting processes.

- **Get Version and Type of Node (Version)**
  https://{hostname}/ise/mnt/api/Version
- **Get Failure Reasons Mapping (FailureReasons)**
  https://{hostname}/ise/mnt/api/FailureReasons
- **Get Session Authentication Status (AuthStatus)**
  https://{hostname}/ise/mnt/api/AuthStatus/MACAddress/{mac}/{seconds}/{number of records per MAC Address}/All
- **Get Session Accounting Status (AcctStatusTT)**
  https://{hostname}/ise/mnt/api/AcctStatusTT/MACAddress/{mac}/{seconds}

For more information:

- For more information about using the troubleshooting APIs in this release, see the *Cisco Identity Services Engine API Reference Guide, Release 1.0.4.*

Note The *Cisco Identity Services Engine API Reference Guide, Release 1.0.4*, also provides information about the supported session management and CoA APIs.

Contacting the Cisco Technical Assistance Center

If you cannot locate the source and potential resolution for a problem in the above sections, contact a Cisco customer service representative for information on how to best proceed with resolving the issue. For Cisco Technical Assistance Center (TAC), see the *Cisco Information Packet* publication that is shipped with your appliance or visit the following website:

http://www.cisco.com/tac/

Before you contact Cisco TAC, make sure that you have the following information ready:

- The appliance chassis type and serial number.
- The maintenance agreement or warranty information (see the *Cisco Information Packet*).
- The name, type of software, and version or release number (if applicable).
- The date you received the new appliance.
- A brief description of the problem or condition you experienced, the steps you have taken to isolate or re-create the problem, and a description of any steps you took to resolve the problem.

Note Be sure to provide the customer service representative with any upgrade or maintenance information that was performed on the Cisco ISE 3300 Series appliance after your initial installation. For site log information, see the "Creating a Site Log" section in the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.0.4*.

Documentation Updates

Table 1 Updates to Cisco Identity Services Engine Troubleshooting Guide, Release 1.0.4

Date	Description
3/18/2013	Added Configure NADs for ISE Monitoring, page 35
9/30/2011	Cisco Identity Services Engine Maintenance Release 1.0.4.573; no content updates made.
8/26/2011	Republished to coincide with Cisco Identity Services Engine Maintenance Release 1.0.4; no content updates made.
8/16/2011	Added Debug Logging for Cisco ISE Agents, page 17 to address CSCtr80776
5/26/2011	Updated CoA Not Initiating on Client Machine, page 3
5/17/2011	Cisco Identity Services Engine, Release 1.0

Related Documentation

Release-Specific Documents

Table 2 lists the product documentation available for the Cisco ISE Release. General product information for Cisco ISE is available at http://www.cisco.com/go/ise. End-user documentation is available on Cisco.com at http://www.cisco.com/en/US/products/ps11640/tsd_products_support_series_home.html.

Table 2 Product Documentation for Cisco Identity Services Engine

Document Title	Location
Release Notes for the Cisco Identity Services Engine, Release 1.0.4	http://www.cisco.com/en/US/products/ps11640/prod_release_notes_list.html
Cisco Identity Services Engine Network Component Compatibility, Release 1.0.4	http://www.cisco.com/en/US/products/ps11640/products_device_support_tables_list.html
Cisco Identity Services Engine User Guide, Release 1.0.4	http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html
Cisco Identity Services Engine Hardware Installation Guide, Release 1.0.4	http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html
Cisco Identity Services Engine Migration Guide for Cisco Secure ACS 5.1 and 5.2, Release 1.0.4	http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html
Cisco Identity Services Engine Sponsor Portal User Guide, Release 1.0.4	http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html
Cisco Identity Services Engine CLI Reference Guide, Release 1.0.4	http://www.cisco.com/en/US/products/ps11640/prod_command_reference_list.html
Cisco Identity Services Engine API Reference Guide, Release 1.0.4	http://www.cisco.com/en/US/products/ps11640/prod_command_reference_list.html
Cisco Identity Services Engine Troubleshooting Guide, Release 1.0.4	http://www.cisco.com/en/US/products/ps11640/prod_troubleshooting_guides_list.html
Regulatory Compliance and Safety Information for Cisco Identity Services Engine, Cisco 1121 Secure Access Control System, Cisco NAC Appliance, Cisco NAC Guest Server, and Cisco NAC Profiler	http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html
Cisco Identity Services Engine In-Box Documentation and China RoHS Pointer Card	http://www.cisco.com/en/US/products/ps11640/products_documentation_roadmaps_list.html

Platform-Specific Documents

Links to Policy Management Business Unit documentation are available on www.cisco.com at the following locations:

- Cisco ISE
  http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html

- Cisco Secure ACS
  http://www.cisco.com/en/US/products/ps9911/tsd_products_support_series_home.html
- Cisco NAC Appliance
  http://www.cisco.com/en/US/products/ps6128/tsd_products_support_series_home.html
- Cisco NAC Profiler
  http://www.cisco.com/en/US/products/ps8464/tsd_products_support_series_home.html
- Cisco NAC Guest Server
  http://www.cisco.com/en/US/products/ps10160/tsd_products_support_series_home.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2011 Cisco Systems, Inc. All rights reserved.